

Amendments to the Specification:

Amend page 27, second full paragraph (lines 13-18) to read as follows:

$\text{Poly_B0} = x^8 \oplus \alpha^{92} \otimes x^7 \oplus \alpha^{229} \otimes x^6 \oplus \alpha^5 \otimes x^5 \oplus \alpha^{95} \otimes x^4 \oplus \alpha^{84} \otimes x^3 \oplus 0 \otimes x^{32} \oplus \alpha^{195} \otimes x \oplus \alpha^{176}$, where $\alpha(X) = \alpha = X$ to obtain the 8-tuple $j_7X^7 + j_6X^6 + j_5X^5 + j_4X^4 + j_3X^3 + j_2X^2 + j_1X + j_0$. The values for the individual coefficient multipliers are as follows:

Amend page 33, last paragraph (lines 12-17) to read as follows:

The non-linear mix functions 161, 162 used to combine two bytes shifted directly from the register A or register B ($\text{RGA}_2/\text{RGA}_4$, $\text{RGB}_3/\text{RGB}_5$) with others that are from the F1 tables:

$$\begin{aligned} g0 &= \text{RGA}'_{0|7} \otimes \text{RGB}'_{1|6} \oplus \text{RGA}_2 \otimes \text{RGB}'_4 \oplus \text{RGA}'_5 \otimes \text{RGB}_3 \\ g1 &= \text{RGA}'_{1|6} \otimes \text{RGB}'_{0|7} + \text{RGA}_4 \otimes \text{RGB}'_2 \oplus \text{RGA}'_3 \otimes \text{RGB}_5 \end{aligned}$$

Amend page 35, first full paragraph (lines 4-16) to read as follows:

The S-box is initialized linearly to $S_0 = 0$, $S_1 = 1$, ..., $S_{255} = 255$. The S-box permutation process can be formulated in accordance with the following relationships:

$$\begin{aligned} &n \text{ from } 0 \text{ to } \text{runup_Cycles} \\ &n = (n \% 256); \\ &Y0' = (g0 + \text{S}_{\text{RGB7|0}} \text{S}_{\text{RGB0|7}} + S_n) \bmod 256 \\ &\text{swap } S_i \text{ and } S_{Y0'} \\ &Y1' = (g1 + \text{S}_{\text{RGA7|0}} \text{S}_{\text{RGA0|7}} + S_n) \bmod 256 \\ &\text{swap } S_i \text{ and } S_{Y1'} \\ &t0 = (S_{g1} + S_{Y0'}) \bmod 256 \\ &t1 = (S_{g0} + S_{Y1'}) \bmod 256 \\ &\mathbf{Y0 = S_{t0} \text{ and } Y1 = S_{t1}} \end{aligned}$$